FIPS 140-1 Cryptographic Modules Validation List

January 10, 2000

The NIST Cryptographic Module Validation (CMV) Program was announced on July 17, 1995. This program validates cryptographic modules for conformance to FIPS 140-1, *Security Requirements for Cryptographic Modules*. In the "Applicability" section of FIPS 140-1, it states that:

> "This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect unclassified information within computer and telecommunication systems (including voice systems) that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. This standard shall be used in designing, acquiring and implementing cryptographic-based security systems within computer and telecommunication systems (including voice systems), operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer or telecommunications system) on behalf of the Federal Government to accomplish a Federal function. Federal agencies which use cryptographic-based security systems for protecting classified information may use those systems for protecting unclassified information in lieu of systems that comply with this standard. Non-Federal government organizations are encouraged to adopt and use this standard when it provides the desired security for protecting valuable or sensitive information."

In the "Implementation Schedule" section of FIPS 140-1, it says that "**After [June 30, 1997], only FIPS 140-1 validated cryptographic modules will be considered as meeting the provisions of this standard.**"

Agencies should require a vendor to provide a copy of a validation certificate, as evidence of CMV Program validation.

*** It is important to note that the items on this list are cryptographic *modules*. This implies that they may *either* be components of a product, *or* complete products in-and-of-themselves. **One should contact a cryptomodule vendor in order to determine what products use the validated cryptomodule.** There is inevitably a larger number of security products available which use a validated cryptomodule, than the number of modules which are found in this list. In addition, **it is possible that other vendors, who are not found in this list, might incorporate a validated cryptomodule from this list into their own products**.

The list below contains those cryptomodules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS 140-1. A validation certificate has been issued for each of the modules in the list below. This list is typically updated either the *day of* or *day after* a certificate is issued.

The module descriptions in the list below are provided by the vendors, and do not imply endorsement by NIST, or the U.S. or Canadian Governments.

FIPS 140-1 Cryptographic Modules Validated Under the CMV Program

#	Vendor	Cryptomodule	Module Type	Validation Date	Level / Description
86	**Motorola, Inc.** Secure Design Center IL02 Room 0509A 1301 East Algonquin Road Schaumburg, IL 60196 http://www.mot.com -Geoff Hobar geoffhobar@motorola.com TEL: (847) 576-9066	**ASTRO-TAC** **Digital Interface Unit (DIU)** **Encryption Module Controller (EMC)** *(when operated in the FIPS mode by selection of the DES algorithm)* (version 3.0A)	**Hardware**	1/5/2000	***Overall Level:*** 1 -Roles and Services: *Level 2* *-FIPS-approved algorithm:* DES (cert.#73). *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-SPFL Multi-chip standalone module. “The ASTRO DIU provides an interface between an analog console and an ASTRO base station or ASTRO-TAC comparator for ASTRO clear and analog two-way radio communications. The DIU EMC is available as an option with ASTRO DIUs to provide encryption capability. The DIU will then support ASTRO encrypted two-way radio communications.”
85	**Entrust Technologies Limited** 750 Heron Road Suite 800 Ottawa, Ontario K1V 1A7 Canada http://www.entrust.com -Marc Laroche TEL: (613) 247-3446 FAX: (613) 247-3450	**Entrust Cryptographic Kernel, V 5.0** *(when operated in the FIPS mode)*	**Software**	1/7/2000	***Overall Level:*** 1 -EMI/EMC: *Level 3* -Roles & Services: *Level 2* -Physical Security: *Level 2* *-Operating System Security:* Tested as meeting **Level 1** for *Microsoft Windows95/98, WindowsNT 3.5 and 3.51, and WindowsNT 4.0 with SP4, SP5, or SP6* (single user mode). *-FIPS-approved algorithms:* DES (cert. #56), DES MAC, DSA/SHA-1 (cert. #10), RSA *(vendor-affirmed)*, Triple DES (DES cert.#56). *-Other algorithms:* RC2, RC4, IDEA, MD5, MD2, RIPEMD-160, HMAC-SHA-1, HMAC-MD5, HMAC-RMD160, CAST, CAST3, CAST5, ECDSA, and D-H key agreement. Multi-chip standalone module. “This module is used in the Entrust family of products.”

84	**Pitney Bowes, Inc.** 35 Waterview Dr Shelton, CT 06484 http://www.pb.com -David Riley rileyda@pb.com TEL: (203) 924-3500 FAX: (203) 924-3385	**ClickStamp™ Online CCV** (ID: CCV assembly, ClickStamp™ Online CCV 1.40.5; KMS, K180034-AAA; IBM 4758-001 certificate #35; CPQ R1.24)	**Hardware**	12/22/1999	***Overall Level:*** **3** -Physical Security: *Level 4 + EFP/EFT* *-FIPS-approved algorithms:* DES (cert. #58), DSA/SHA-1 (cert. #23), Triple DES. *-Other algorithms:* RSA. Multi-chip embedded module. "The module provides security services to support the secure accounting and cryptographic functions necessary for value evidencing of electronic transactions, such as the United States Postal Service Information-Based Indicium Program (USPS IBIP)."
83	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Mina Paik Paik.Mina@cylink.com	**Cylink Link Encryptor NRZ E1-75Ω and Link Encryptor RS-232** (Firmware versions 1.25 and 1.26)	**Hardware**	12/22/1999	***Overall Level:*** **2** -Physical Security: *Level 3* -Software Security: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #26); DSA/SHA-1 (cert. #5), Triple DES (DES certs. #11 and #26). *-Other algorithms:* Diffie-Hellman Key Agreement. Multi-chip standalone module. "Cylink Link Encryptors secure sensitive data transmitted over high-speed, point-to-point communication links. The system supports synchronous, full-duplex data rates up to 2 Mbps over public and private data networks."
82	**Motorola, Inc.** Secure Design Center IL02 Room 0509A 1301 East Algonquin Rd Schaumburg, IL 60196 http://www.mot.com -Geoff Hobar geoff.hobar@motorola.com TEL: (847) 576-9066 FAX: (847) 538-2770	**ASTRO Subscriber Encryption Module** *(when operated in the FIPS mode by selecting the DES algorithm)* (Software Version 3.40)	**Hardware**	12/22/1999	***Overall Level:*** **1** -Roles and Services: *Level 2* -Software Security: *Level 3* *-FIPS-approved algorithm:* DES, Triple DES *-Other algorithms:* DES-XL, DVP-XL, DVI-XL, DVI-SPFL Multi-chip embedded module. "Encryption modules used in Motorola Astro™ family of radios. Provides secure voice and data capabilities as well as APCO Over-the-Air-Rekeying and advanced key management."

81	**IBM Corp.** 522 South Road Mail Stop P339 Poughkeepsie, NY 12601-5400 http://www.ibm.com/security/ products -Helmy El-Sherif TEL: (914) 435-7033 FAX: (914) 435-4092 helmy@us.ibm.com	**IBM 4758 PCI Cryptographic Coprocessor** (Miniboot Layers 0 and 1) (ID: PN IBM 4758-013, Miniboot 0 version B, Miniboot 1 version B)	**Hardware**	11/29/1999	***Overall Level:*** **3** *-Physical Security: Level 3 + EFP/EFT* *-Cryptographic Module Design: Level 4* *-Module Interfaces: Level 4* *-Roles and Services: Level 4* *-Finite State Machine Model: Level 4* *-Software Security: Level 4* *-EMI/EMC: Level 4* *-Self-Tests: Level 4* *-Key Management: Level 4* *-FIPS-approved algorithms:* DES (cert. #41); DSA/SHA-1 (cert. #16); Triple DES. *-Other algorithms:* RSA. Multi-chip embedded module. "The 4758 is a tamper-responding, programmable, cryptographic PCI card, containing CPU, encryption hardware, RAM, EEPROM, hardware random number generator, time of day clock, firmware, and software."
80	**Dallas Semiconductor, Inc.** 4401 Beltwood Parkway Dallas, TX 75244-3292 http://www.iButton.com -Mr. Dennis Jarrett TEL: (972) 371-4416 Dennis.Jarrett@dalsemi.com	**DS1954B -006** **Cryptographic iButton™** *(ID: B7-V1.02)* *(when using vendor-initialized SHA-1 in transaction group 1)*	**Hardware**	11/29/1999	***Overall Level:*** **3** -Physical Security: *Level 3 + EFP* *-FIPS-approved algorithms:* SHA-1 (cert. #8). *-Other algorithms:* MD5, RSA. Multi-chip standalone module. "Inside the steel perimeter, the secure accounting and cryptographic services are performed to meet the requirements of the United States Postal Service Information Based Indicia Program. See Cert. #41 below."
79	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Jennifer Mitchell TEL: (847) 576-7251	**KVL 3000** *(when operated in the FIPS mode by selection of the DES algorithm)* (Hardware version CLN6738B; Firmware version R02.50.00)	**Hardware**	11/29/1999	***Overall Level:*** **1** *-FIPS-approved algorithm:* DES (cert. #5) *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-SPEL. Multi-chip standalone module. "The KVL3000 Key Variable Loader is a battery-powered portable unit used to create, store, and transfer encryption keys used by Motorola's secure communications products. The KVL3000 supports the following Motorola encryption protocols: SECURENET™, Advanced SECURENET™, ASTRO™, and ASTRO™25 systems."

78	**SPYRUS, Inc.** 10320 Little Patuxent Parkway Suite 802 Columbia, MD 21044-3312 http://www.spyrus.com -James K. Wharton (410) 964-6400 jwharton@spyrus.com	**LYNKS Privacy Card** *(For services provided by the FIPS-approved algorithms listed [in the description column])* (Hardwareversion 2.0; Firmware version 1.2)	**Hardware**	11/29/1999	***Overall Level:*** **2** -*FIPS-approved algorithms:* DES (cert.#50), SKIPJACK (cert. #1), DSA/SHA-1 (cert. #1), Triple DES. -*Other algorithms:* RSA, Diffie-Hellman Key Agreement, KEA, MD5. Multi-chip standalone module. “The SPYRUS family of LYNKS Privacy Card tokens provides high performance, high assurance cryptographic processing in a personal, portable PC card form factor. The LYNKS Privacy Card product enables security-critical capabilities such as user authentication, message privacy and integrity, authentication, and secure storage in rugged, tamper-evident hardware.”
77	**Attachmate Corp.** 424 Wards Corner Road Loveland, OH 45140 http://www.attachmate.com -Bill Evans TEL: (513) 794-8140 BillEv@attachmate.com	**CryptoConnect ETS** *(For services provided by the FIPS-approved algorithms[listed in the description column])* (Version 2.2.1)	**Software**	11/29/1999	***Overall Level:*** **1** -*EMI/EMC: Level 3* -*Operating System Security:* Tested as meeting **Level 1** with *Microsoft Windows95, Windows98, and WindowsNT 4.0, with SP3 or later* (single-user mode). -*FIPS-approved algorithms:* DES (cert. #46), Triple DES, DSA/SHA-1 (cert. #18) -*Other algorithms:* RSA (encryption), RC2, RC4. Multi-chip standalone module. “CryptoConnect ETS is an INFOConnect transport system that provides encryption of all data between Attachmate’s PEP/UTS client and Unisys 2200/ClearPath/IX Systems.”

76	**Microsoft Corporation** One Microsoft Way Redmond, WA 98052-6399 http://www.microsoft.com -Tiffany Treacy tiffanyj@microsoft.com	**Base DSS Cryptographic Provider,** **Base Cryptographic Provider,** **DSS/Diffie-Hellman Enchanced Cryptographic Provider, and Enhanced Cryptographic Provider** *(For services provided by the FIPS-approved algorithms [listed in the description column])* (version 5.0.2150.1)	**Software**	11/9/1999	***Overall Level:* 1** *-EMI/EMC: Level 3* *-Operating System Security:* Tested as meeting **Level 1** with *Microsoft Windows2000* (operated in single-user mode). *-FIPS-approved algorithms:* DES (certs. #65, 66, 67, 68); Triple DES; DSA/SHA-1 (cert. #28, 29); RSA (vendor-affirmed). *-Other algorithms:* RC2, RC4, MD2, MD4, MD5, and Diffie-Hellman. Multi-chip standalone module. “These are general-purpose software-based cryptomodules. They provide services that enable application developers to utilize several different cryptographic algorithms and functions via the Microsoft CryptoAPI without knowing the underlying implementation.”
75	**Microsoft Corporation** One Microsoft Way Redmond, WA 98052-6399 http://www.microsoft.com -Tiffany Treacy tiffanyj@microsoft.com	**Base DSS Cryptographic Provider,** **Base Cryptographic Provider,** **DSS/Diffie-Hellman Enchanced Cryptographic Provider, and Enhanced Cryptographic Provider** *(For services provided by the FIPS-approved algorithms [listed in the description column])* (versions 5.0.1877.6 and 5.0.1877.7)	**Software**	11/9/1999	***Overall Level:* 1** *-EMI/EMC: Level 3* *-Operating System Security:* Tested as meeting **Level 1** with *Microsoft Windows95 and Windows98* (operated in single-user mode). *-FIPS-approved algorithms:* DES (certs. #61, 62, 63, 64); Triple DES; SHA-1 (certs. #20, 21); DSA/SHA-1 (cert. #25, 26); RSA (vendor-affirmed). *-Other algorithms:* RC2, RC4, MD2, MD4, MD5, and Diffie-Hellman. Multi-chip standalone module. “These are general-purpose software-based cryptomodules. They provide services that enable application developers to utilize several different cryptographic algorithms and functions via the Microsoft CryptoAPI without knowing the underlying implementation.”

74	**RedCreek Communications** 3900 Newpark Mall Rd. Newark, CA 94056 http://www.redcreek.com -Chris McComb TEL: (510) 745-3900 cmccomb@redcreek.com	**Personal Ravlin** (Hardware v 08; Firmware v 3.32 Standard) *(For services provided by the FIPS-approved algorithms[listed in the description column])*	**Hardware**	11/4/1999	***Overall Level:*** **2** *-FIPS-approved algorithms:* DES (cert. #53), Triple DES, DSA/SHA-1 (cert. #22) *-Other algorithms:* MD5. Multi-chip standalone module. "The Personal Ravlin is a cost-effective network security solution. It addresses the needs of individual remote users who access corporations via cable, xDSL, and ISDN modems. It is also an ideal solution for network administrators who seek to establish private communications within a corporate intranet by providing security at the desktop level."
73	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Mina Paik Paik.Mina@cylink.com	**Cylink Link Encryptor NRZ-L** (Firmware v1.25 and v1.26)	**Hardware**	10/25/1999	***Overall Level:*** **2** -Physical Security: *Level 3* -Software Security: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #26); DSA/SHA-1 (cert. #5). *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), and Diffie-Hellman Key Agreement. Multi-chip standalone module. "Cylink Link Encryptors secure sensitive data transmitted over high-speed, point-to-point communication links. The system supports synchronous, full-duplex data rates up to 2 Mbps over public and private data networks."
72	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Mina Paik Paik.Mina@cylink.com	**Cylink Link Encryptor NRZ-H** (Firmware v1.25 and v1.26)	**Hardware**	10/25/1999	***Overall Level:*** **2** -Physical Security: *Level 3* -Software Security: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #26); DSA/SHA-1 (cert. #5). *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), and Diffie-Hellman Key Agreement. Multi-chip standalone module. "Cylink Link Encryptors secure sensitive data transmitted over high-speed, point-to-point communication links. The system supports synchronous, full-duplex data rates up to 2 Mbps over public and private data networks."

71	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -John Parker Parker.John@cylink.com	**Cylink Frame Encryptor CFE-L** *(when operated in the FIPS mode)* (Firmware v4.02 and Hardware revisions 4 and 5)	**Hardware**	9/13/1999	***Overall Level:*** **3** -Module Interfaces: *Level 3** -Roles and Services: *Level 3** *(Level 3 - Console interface disabled; Level 2 - Console interface enabled.) *-FIPS-approved algorithms:* DES (certs. #11, #20); DSA/SHA-1 (cert. #5). -*Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), and Diffie-Hellman Key Agreement. Multi-chip standalone module. “Cylink Frame Encryptors secure sensitive data transmitted over high-speed, Frame Relay communication links.”
70	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -John Parker Parker.John@cylink.com	**Cylink Frame Encryptor CFE-H** *(when operated in the FIPS mode)* (Firmware v4.02 and Hardware revisions 4 and 5)	**Hardware**	9/13/1999	***Overall Level:*** **3** -Module Interfaces: *Level 3** -Roles and Services: *Level 3** *(Level 3 - Console interface disabled; Level 2 - Console interface enabled.) *-FIPS-approved algorithms:* DES (certs. #11, #20); DSA/SHA-1 (cert. #5). -*Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), and Diffie-Hellman Key Agreement. Multi-chip standalone module. “Cylink Frame Encryptors secure sensitive data transmitted over high-speed, Frame Relay communication links.”
69	**Mykotronx, Inc.** 357 Van Ness Way Suite 200 Torrance, CA 90501 http://www.rainbow.com/mykoweb/ -Kevin Cook TEL: (310) 533-8100 FAX: (310) 533-0527 kcook@myko.rainbow.com	**FORTEZZA Crypto Card** (Part Number 650000-2)	**Hardware**	9/13/1999	***Overall Level:*** **2** -EMI/EMC: *Level 3* *FIPS-approved algorithms:* DSA/SHA-1 (cert. #2), Skipjack (cert. #2). *Other algorithms:* KEA Multi-chip standalone module. “The Mykotronx FORTEZZA card is a PC Card hardware token for advanced cryptography and authorization methods. The card incorporates the National Security Agency-certified CAPSTONE RISC-based cryptographic processor.”

68	**Microsoft Corporation** One Microsoft Way Redmond, WA 98052-6399 http://www.microsoft.com -Tiffany Treacy tiffanyj@microsoft.com	**Base Cryptographic Provider, Enhanced Cryptographic Provider, Base DSS Cryptographic Provider, and DSS/Diffie-Hellman Enchanced Cryptographic Provider** *(For services provided by the FIPS-approved algorithms [listed in the description column] and Triple DES)* (versions 5.0.1877.6 and 5.0.1877.7)	**Software**	9/13/1999	***Overall Level:*** **1** *-EMI/EMC: Level 3* *-Operating System Security:* Tested as meeting **Level 1** with *Microsoft WindowsNT 4.0 with Service Pack 6* (operated in single-user mode). *-FIPS-approved algorithms:* DES (certs. #61, 62, 63, 64); SHA-1 (certs. #20, 21); DSA/SHA-1 (cert. #25, 26); RSA (vendor-affirmed). *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use); RC2, RC4, MD2, MD4, MD5, and Diffie-Hellman. Multi-chip standalone module. "These are general-purpose software-based cryptomodules. They provide services that enable application developers to utilize several different cryptographic algorithms and functions via the Microsoft CryptoAPI without knowing the underlying implementation."
67	**Certicom Corporation** 200 Matheson Blvd. West Suite 103 Mississauga, Ontario L5R 3L7 CANADA http://www.certicom.com -Alex Chartier TEL: (905) 507-4220 FAX: (905) 507-9406 achartie@certicom.com	**CERTIFAX Fax Encryptor CF3102** *(When operated in the FIPS mode using the FIPS-approved algorithms [listed in the description column] and Triple DES)* (not valid for FS1000 interoperability) (ID: firmware version 2.21)	**Firmware**	9/13/1999	***Overall Level:*** **3** *-Self-Tests: Level 4* *-FIPS-approved algorithms:* DES (cert. #42); SHA-1 (cert. #15). *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use); ECDSA; ECMQV2; Discrete Log Diffie-Hellman. Multi-chip standalone module. CERTIFAX 3000 secures sensitive facsimile communications from inadvertent or intentional disclosure. CERTIFAX ensures faxes get to the intended recipient every time, that the contents are never disclosed to unauthorized parties, that the sender is who it claims to be, and that the message is always kept private and unaltered. CERTIFAX provides two-way authentication using Certicom's Elliptic Curve Cryptography, and strong encryption using Triple DES. CERTIFAX's secure mailbox memory provides storage and retrieval for incoming faxes, and CERTIFAX can support up to 99 secure Virtual Private Fax Networks. The CF3102 also implements a non-FIPS mode for communications with Certicom's Legacy Fax Secret 1000 fax encryptor.

66	**Racal AirTech Ltd. / Racal Guardata, Inc.** 1601 N. Harrison Pkwy. Sunrise, FL 33323 http://www.racalitsec.com -Cindy Provin TEL: (888) 744-4976 americas.sales@racalitsec.com security@racalitsec.com itsecurity@racal.com.uk	**Datacryptor® 2000 (DC2K) Link / Channelized / Frame Relay** (Hardware Version Issue 2 Motherboard; Software Version 1.02.36) *(when key zeroization is enabled)*	**Hardware**	9/8/1999	***Overall Level:*** **3** *-FIPS-approved algorithms:* DES (cert. #57), DSA/SHA-1 (cert. #24) *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), Diffie-Hellman Key Agreement. Multi-chip standalone module.
65	**RedCreek Communications** 3900 Newpark Mall Rd. Newark, CA 94056 http://www.redcreek.com -Chris McComb TEL: (510) 745-3900 cmccomb@redcreek.com	**Ravlin 10** (Hardware v 09; Software v 3.32 Radius) *(For services provided by the FIPS-approved algorithms[listed in the description column] and Triple DES)*	**Hardware**	9/8/1999	***Overall Level:*** **2** *-FIPS-approved algorithms:* DES (cert. #53), DSA/SHA-1 (cert. #22) *-Other algorithms:* TripleDES (allowed for U.S. and Canadian Government use), MD5. Multi-chip standalone module. The Ravlin 10/5100 is a network security solution that performs encryption and decryption with a throughput of the theoretical maximum of Ethernet (or “wire” speed). Network administrators use it to establish private communications within secure intranets (between corporate divisions, workgroups, branch offices, and individuals) or within secure extranets (between customers, suppliers, and strategic partners). This may be done over private or public IP networks.

64	**Network Associates, Inc.** 3965 Freedom Circle Santa Clara, CA 95054 http://www.nai.com -Mark J. McArdle TEL: (408) 346-5189 FAX: (408) 346-3399 mark_mcardle@nai.com	**PGP Cryptographic SDK, Version 1.5** *(when operated in the FIPS mode using the FIPS-approved algorithms listed [in the description column] and Triple DES)*	**Software**	8/26/1999	***Overall Level:*** 2 -*Operating System Security:* Tested as meeting **Level 2** with *Compaq DeskPro 5/166 w/WindowsNT Workstation 3.51 w/Service Pack 4* (ITSEC-rated). -*FIPS-approved algorithms:* DES (cert. #40), DSA/SHA-1 (cert. #20) -*Other algorithms:* TripleDES (allowed for U.S. Government use), RSA, El Gamal, CAST5, IDEA, MD5, RIPEMD60, HMAC, Shamir Threshold Secret Sharing. Multi-chip standalone module. The PGP SDK provides all cryptographic and key management functionality for the PGP suite of products, including PGP Desktop Security, PGPnet VPN Client, PGPdisk and the PGP Certificate Server. This is a high-level toolkit for use with C/C++ applications on Windows. It also supports PGP/MIME, TLS, Certificate Server management, LDAP, and Blakely-Shamir Key Splitting, as well as many user interface components for simple integration into other applications. PGP SDK implements only strong cryptography, and the source code is published in book form for peer review.
63	**Dallas Semiconductor, Inc.** 4401 Beltwood Parkway Dallas, TX 75244-3292 http://www.iButton.com -Mr. Dennis Jarrett TEL: (972) 371-4416 Dennis.Jarrett@dalsemi.com	**DS1954B Cryptographic iButton™** *(ID: B7-V1.02)* *(when using vendor-initialized SHA-1 in transaction group 1)*	**Hardware**	8/26/1999	***Overall Level:*** 3 -Physical Security: *Level 3 + EFP* -*FIPS-approved algorithms:* SHA-1 (cert. #8) -*Other algorithms:* MD5, RSA Multi-chip standalone module. Inside the steel perimeter, the secure accounting and cryptographic services are performed to meet the requirements of the United States Postal Service Information Based Indicia Program. See Cert. #41 below.

62	**Francotyp-Postalia** Triftweg 21-26 D-16547 Birkenwerder Germany http://www.francotyp.com -Andreas Wagner a.wagner@francotyp.com	**Francotyp-Postalia Security Module (FPSM)** (Software Version 1.1; Hardware Version 1.0)	**Hardware**	8/17/1999	***Overall Level:*** **2** -Physical Security: *Level 3* -Key Management: *Level 3* -Module Interfaces: *Level 3* -Software Security: *Level 3* -Self-Tests: *Level 3* -EMI/EMC: *Level 3* *FIPS-approved algorithms:* DES (cert. #59) *Other algorithms:* TripleDES (allowed for U.S. Government use) Multi-chip embedded module. The FPSM is a multi-chip embedded cryptomodule. The FPSM is embedded in Postage Meters and provides security services to support the secure accounting and cryptographic functions necessary to implement a value evidencing apparatus.
61	**Mykotronx, Inc.** 357 Van Ness Way Suite 200 Torrance, CA 90501 http://www.rainbow.com/ mykoweb/index.htm -Richard Macherzak rmacherzak@myko.rainbow.com	**Palladium Secure Modem / FORTEZZA CryptoCard** (Hardware Version 1.5; Software Version p1.81)	**Hardware**	8/11/1999	***Overall Level:*** **1** -EMI/EMC: *Level 3* *FIPS-approved algorithms:* DSA/SHA-1 (cert. #2), Skipjack (cert. #2) Multi-chip standalone module.
60	**Microsoft Corporation** One Microsoft Way Redmond, WA 98052-6399 http://www.microsoft.com -Charlie Chase charliec@microsoft.com	**DSS/Diffie-Hellman Enhanced Cryptographic Provider** *(For services provided by the FIPS-approved algorithms [listed in the description column] and Triple DES)* (software version 5.0.1998.1)	**Software**	8/5/1999	***Overall Level:*** **1** *-EMI/EMC: Level 3* *-Operating System Security:* Tested as meeting **Level 1** with *Microsoft WindowsNT 4.0 with Service Pack 4* (operated in single-user mode). *-FIPS-approved algorithms:* DES (cert. #45); DSA/SHA-1 (cert. #17). *-Other algorithms:* TripleDES (allowed for U.S. Government use); RC2, RC4, MD5, and Diffie-Hellman. Multi-chip standalone module. Microsoft's DSSENH is a general-purpose software-based cryptographic module. It provides services that enable application developers to utilize several different cryptographic algorithms and functions via the Microsoft CryptoAPI without knowing the underlying implementation..

59	**Certicom Corporation** 200 Matheson Blvd. West Suite 103 Mississauga, Ontario L5R 3L7 CANADA http://www.certicom.com -Alex Chartier TEL: (905) 507-4220 FAX: (905) 507-9406 achartie@certicom.com	**CERTIFAX Fax Encryptor CF3002 and CF3003** *(When operated in the FIPS mode)* (ID: firmware version 2.20)	**Firmware**	8/5/1999	***Overall Level:* 3** *-Self-Tests: Level 4* *-FIPS-approved algorithms:* DES (cert. #42); SHA-1 (cert. #15). *-Other algorithms:* TripleDES (allowed for U.S. Government use); ECDSA; ECMQV2. Multi-chip standalone module. CERTIFAX 3000 secures sensitive facsimile communications from inadvertent or intentional disclosure. CERTIFAX ensures faxes get to the intended recipient every time, that the contents are never disclosed to unauthorized parties, that the sender is who it claims to be, and that the message is always kept private and unaltered. CERTIFAX provides two-way authentication using Certicom's Elliptic Curve Cryptography, and strong encryption using Triple DES. CERTIFAX's secure mailbox memory provides storage and retrieval for incoming faxes, and CERTIFAX can support up to 99 secure Virtual Private Fax Networks.
58	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**LunaCA**[3] *(For services provided by the FIPS-approved algorithms listed [in the description column], and Triple DES)* (firmware version 3.2)	**Hardware**	8/5/1999	***Overall Level:* 3** *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13); and RSA (vendor-affirmed). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, MD2, MD5, and D-H key agreement. Multi-chip standalone module.
57	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**LunaCA** *(For services provided by the FIPS-approved algorithms listed [in the description column], and Triple DES)* (firmware version 3.2)	**Hardware**	8/5/1999	***Overall Level:* 2** -Software Security: *Level 3* -Self Tests: *Level 3* *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13); and RSA (vendor-affirmed). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, RC5, MD2, MD5, and D-H key agreement. Multi-chip standalone module. LunaCA is a hardware crypto engine for identification and authentication (I&A) and digital signing; supports encryption/decryption and random number generation. Its target is certification authority systems that require a secure key generation and signing capability. LunCA is a token based on the PCMCIA standard - now known as PC Card.

56	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**Luna2** *(For services provided by the FIPS-approved algorithms listed [in the description column], and Triple DES)* (firmware version 3.2)	**Hardware**	8/8/1999	***Overall Level:*** 2 -Software Security: *Level 3* -Self Tests: *Level 3* *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13); and RSA (vendor-affirmed). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, RC5, MD2, MD5, and D-H key agreement. Multi-chip standalone module. Luna2 is a hardware crypto engine for identification and authentication (I&A) and digital signing; supports encryption/decryption and random number generation. Its target is certification authority systems that require a secure key generation and signing capability. Luna2 is a token based on the PCMCIA standard - now known as PC Card.
55	**Certicom Corporation** 200 Matheson Blvd. West Mississauga, Ontario L5R 3L7 CANADA http://www.certicom.com -James Wright TEL: (510) 780-5442 jwright@certicom.com	**Elliptic Curve Security Module (CLv)** (hardware version R4, firmware version R1.4.1)	**Hardware**	6/21/1999	***Overall Level:*** 2 *-FIPS-approved algorithms:* DES (cert. #51); DSA/SHA-1 (cert. #19). *-Other algorithms:* TripleDES (allowed for U.S. Government use); EC-DH. Multi-chip embedded module.
54	**TimeStep Corporation** 359 Terry Fox Drive. Kanata, Ontario K2K 2E7 CANADA http://www.timestep.com -Brett Howard TEL: (613) 599-3610 x4554 FAX: (613) 599-3617 bretth@timestep.com	**PERMIT/Gate 2520™ Cryptographic Module** *(when operated in the FIPS mode)* (Hardware version 1.20)	**Hardware**	6/15/1999	***Overall Level:*** 2 *-Software Security: Level 3* *-FIPS-approved algorithms:* DES; DSA/SHA-1 (cert. #21). *-Other algorithms:* TripleDES (allowed for U.S. Government use), MD5.. Multi-chip standalone module. PERMIT/Gate 2520™ is a high-speed VPN component of the PERMIT™ Enterprise product suite. It is a tamper-resistant gateway that secures data communications for Intranets, Extranets, and Internet remote access. The 2520 has 4Mbps throughput.

53	**TimeStep Corporation** 359 Terry Fox Drive. Kanata, Ontario K2K 2E7 CANADA http://www.timestep.com -Brett Howard TEL: (613) 599-3610 x4554 FAX: (613) 599-3617 bretth@timestep.com	**PERMIT/Gate 4520™ Cryptographic Module** *(when operated in the FIPS mode)* (Hardware version 1.20)	**Hardware**	6/15/1999	***Overall Level:*** 2 *-Software Security: Level 3* *-FIPS-approved algorithms:* DES; DSA/SHA-1 (cert. #21). *-Other algorithms:* TripleDES (allowed for U.S. Government use), MD5. Multi-chip standalone module. PERMIT/Gate 4520™ is a high-speed VPN component of the PERMIT™ Enterprise product suite. It is a tamper-resistant gateway that secures data communications for Intranets, Extranets, and Internet remote access. The 4520 has 10Mbps throughput. The 4520 is the same as the 2520, except that the 4520 has a faster CPU, running at a higher bus frequency.
52	**Certicom Corporation** 200 Matheson Blvd. West Suite 103 Mississauga, Ontario L5R 3L7 CANADA http://www.certicom.com -Alex Chartier TEL: (905) 507-4220 FAX: (905) 507-9406 achartie@certicom.com	**CERTIFAX Fax Encryptor CF3001** *(When operated in the FIPS mode)* (ID: firmware version 2.2)	**Hardware**	6/15/1999	***Overall Level:*** 3 *-Self-Tests: Level 4* *-FIPS-approved algorithms:* DES (cert. #42); SHA-1 (cert. #15). *-Other algorithms:* TripleDES (allowed for U.S. Government use); ECDSA; ECMQV2. Multi-chip standalone module. CERTIFAX 3000 secures sensitive facsimile communications from inadvertent or intentional disclosure. CERTIFAX provides two-way authentication using Certicom's Elliptic Curve Cryptography, and strong encryption using Triple DES. CERTIFAX can support up to 99 secure Virtual Private Fax Networks.
51	**Pitney Bowes, Inc.** 1 Elmcroft Rd. Stamford, CT 06926-0700 http://www.pb.com -Frederick W. Ryan, Jr. TEL: (203) 924-3500 FAX: (203) 924-3385 ryanfw@pb.com	**Clickstamp** *(Validated only for the DES MAC authenticated services: Credit, Put IBIP Data, and Zeroize Keys)* (Part #P200, Version AAA)	**Hardware**	5/10/1999	***Overall Level:*** 3 *-FIPS-approved algorithms:* DES (cert. #35); SHA-1 (cert. #11). *-Other algorithms:* RSA. Multi-chip standalone module. The module provides security services to support the secure accounting and cryptographic functions necessary for value evidencing of electronic transactions, such as the United States Postal Service Information-Based Indicium Program (USPS IBIP).

50	**RSA Data Security, Inc.** 2955 Campus Drive Suite 400 San Mateo, CA 94403 http://www.rsa.com -Mike Vergera mvergera@rsa.com	**BSAFE Crypto-C Toolkit, Version 4.11** *(For services provided by the FIPS-approved algorithms listed [in the description column] and Triple DES)*	**Software**	4/29/1999	***Overall Level:*** 1 *-EMI/EMC: Level 3* *-FIPS-approved algorithms:* DES (cert. #46), DSA/SHA-1 (cert. #18) *-Other algorithms:* TripleDES (allowed for U.S. Government use), RSA, MD2, MD5, HMAC, DESX, RC2, RC4, Elliptic Curve (F2&Fp), Elliptic Curve Encryption Scheme, Elliptic Curve DSA, and Bloom-Shamir. Multi-chip standalone module. Cryptographic Toolkit provides cryptographic services to calling applications.
49	**Intel Network Systems, Inc.** 2 Eva Road, Suite 220 Toronto, Ontario M9C 2A8 Canada http://www.shiva.com -Robert Eng TEL: (416) 622-8987 FAX: (416) 622-7577 reng@shiva.com	**LAN Rover VPN Gateway (LRVG) V6.59** (firmware version V6.59)	**Hardware**	4/28/1999	***Overall Level:*** 2 *-Software Security: Level 3* *-EMI/EMC: Level 3* *-FIPS-approved algorithms:* DES, SHA-1 (cert. #18) *-Other algorithms:* TripleDES (allowed for U.S. Government use). Multi-chip standalone module. The LRVG is a network packet encryption device which incorporates firewall and tunneling functionality compatible with a variety of protocols over Ethernet, V.35, and RS-232.
48	**SPYRUS, Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick TEL: (410) 964-6400 BBialick@spyrus.com	**FORTEZZA Crypto Card, v0.5** (firmware version 0.5)	**Hardware**	4/23/1999	***Overall Level:*** 2 *-FIPS-approved algorithms:* SKIPJACK (cert. #1), DSA/SHA-1 (cert. #1) *-Other algorithms:* KEA. Multi-chip standalone module. SPYRUS's FORTEZZA is a PC Card that is used to provide cryptographic services.
47	**Netscape Communications Corporation** 6905 Rockledge Dr., Suite 820 Bethesda, MD 20817 `http://www.netscape.com` -Frank Hecker Netscape Govt. Sales TEL: (301) 571-3907 FAX: (301) 571-3915 fips@netscape.com	**Netscape Security Module 1.01** *(when operated in the FIPS mode)* (ID: *fipscm_v1.01*)	**Software**	3/17/1999	***Overall Level:*** 2 *-Physical Security:* **Level 2** met when correctly implementing the tamper evident mechanism specified in the security policy. *-Operating System Security:* Tested as meeting **Level 2** with *Sun Ultra-5 w/ Sun Trusted Solaris version 2.5.1* (ITSEC-rated). *-FIPS-approved algorithms:* DES (certs. #33, #34); DSA and SHA-1 (cert. #14); RSA (vendor affirmed). *-Other algorithms:* Triple DES (allowed for U.S. Government use), RC2, RC4, MD2, MD5. Security module used in various Netscape products.

46	**SPYRUS, Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick (410) 964-6400 BBialick@spyrus.com	**LYNKS Metering Device (LMD)** (firmware version 9012)	**Hardware**	3/17/1999	***Overall Level:*** 2 -Physical Security: *Level 3*+EFT *-FIPS-approved algorithms:* SKIPJACK (cert. #1), DSA/SHA-1 (cert. #1) Multi-chip standalone module.
45	**Netscape Communications Corporation** 6905 Rockledge Dr., Suite 820 Bethesda, MD 20817 http://www.netscape.com -Frank Hecker Netscape Govt. Sales TEL: (301) 571-3907 FAX: (301) 571-3915 fips@netscape.com	**Netscape Security Module 1.01** *(when operated in the FIPS mode)* (ID: *fipscm_v1.01*)	**Software**	3/17/1999	***Overall Level:*** 1 *-Operating System Security:* meets **Level 1** for *WindowsNT 4.0 workstation* (operated in single user mode). *-FIPS-approved algorithms:* DES (certs. #33, #34); DSA and SHA-1 (cert. #14); RSA (vendor affirmed). *-Other algorithms:* Triple DES (allowed for U.S. Government use), RC2, RC4, MD2, MD5. Security module used in various Netscape products.
44	**Ericsson** MVR, Room 2700 Mountain View Road Lynchburg, VA 24502 http://www.ericsson.com -Victoria Repice victoria_repice@ena-east.ericsson.se	**Aegis M-RK II System and Scan** (Part#: 344A937P253; 344A3937P273, Software Load #CXC 112 1279/1, version M2G30408) Model Numbers: PK2PGE, PK3PGE, PK2PGA, PK3PGA, PK2PEE, PK3PEE, PK2PEA, PK3PEA	**Hardware**	3/4/1999	***Overall Level:*** 1 *-FIPS-approved algorithms:* DES. Multi-chip standalone module.
43	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Dale Witt dwitt@cylink.com	**Turbo Crypto Card (TCC), v09, 14.04** (Part#: AB-14094-050-09)	**Hardware**	2/17/99	***Overall Level:*** 1 -EMI/EMC: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #20); DSA/SHA-1 (cert. #5). *-Other algorithms:* Diffie-Hellman. Multi-chip embedded module. Turbo Crypto Card is used in a variety of Cylink's host encryption products, including the Secure Frame Unit (SFU) and the Secure Domain Unit (SDU).
42	**Fortress Technologies** 2701 North Rocky Point Dr. Suite 650 Tampa, FL 33607 http://www.fortresstech.com -Dr. Eva Bozoki eva@fortresstech.com	**Segmented NetFortress™ GVPN-S** *(Version -1)* *(when factory configured in FIPS mode)*	**Hardware**	1/27/1999	***Overall Level:*** 2 -EMI/EMC: *Level 3* *-FIPS-approved algorithms:* DES (cert. #23) *-Other algorithms:* TripleDES (allowed for U.S. Government use), IDEA. Multi-chip standalone module. VPN Encryptor.

41	**Dallas Semiconductor, Inc.** 4401 Beltwood Parkway Dallas, TX 75244-3292 http://www.iButton.com -Mr. Dennis Jarrett TEL: (972) 371-4416 Dennis.Jarrett@dalsemi.com	**DS1954B Cryptographic iButton™** *(ID: B4-V1.02)* *(when using vendor-initialized SHA-1 in transaction group 1)*	**Hardware**	1/26/1999	***Overall Level:*** 3 *-Physical Security: Level 3 + EFP* *-FIPS-approved algorithms:* SHA-1 (cert. #8) *-Other algorithms:* MD5, RSA Multi-chip standalone module. Provides hardware cryptographic services (e.g., secure private key storage, high-speed math accelerator for 1024-bit public key crypto, hashing). Services are provided using a single silicon chip packaged in a 16mm stainless steel case. Can be worn or attached to an object for info at point of use. Can withstand harsh outdoor environments and is durable for everyday wear.
40	**IBM Corp.** MS/P371 522 South Road Poughkeepsie, NY 12601-5400 http://www.ibm.com/security/products -Randall J. Easter TEL: (914) 435-8313 FAX: (914) 435-1858 reaster@us.ibm.com -Phil C. Yeh TEL: (914) 435-7661 FAX: (914) 432-9413 pyeh@us.ibm.com	**IBM S/390 CMOS Cryptographic Coprocessor** *(When configured for External Key Entry)* (ID: IBM Part #s 88H3637 and 29L3659)	**Hardware**	1/7/1999	***Overall Level:*** 4 *-FIPS-approved algorithms:* DES (cert. #7, 29); DSA/SHA-1 (cert. #4, 12); RSA (internal use) *-Other algorithms:* TripleDES (allowed for U.S. Government use); CDM; MDC-2; MDC-4; D-H key agreement; ANSI: X3.106, X9.9, X9.19. Single-chip module. Encryption module for S/390 CMOS Enterprise Server family.
39	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**Luna2** *(For services provided by the FIPS-approved algorithms list [in the description column], and Triple DES)* (firmware version 2.2)	**Hardware**	12/8/98	***Overall Level:*** 2 -Software Security: *Level 3* -Self Tests: *Level 3* *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, RC5, MD2, MD5, RSA, and D-H key agreement. Multi-chip standalone module. Luna2 is a hardware crypto engine for identification and authentication (I&A) and digital signing; supports encryption/decryption and random number generation. Its target is certification authority systems that require a secure key generation and signing capability. Luna2 is a token based on the PCMCIA standard - now known as PC Card.

38	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**LunaCA** *(For services provided by the FIPS-approved algorithms list [in the description column], and Triple DES)* (firmware version 2.2)	**Hardware**	12/8/98	***Overall Level:*** **2** -Software Security: *Level 3* -Self Tests: *Level 3* *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, RC5, MD2, MD5, RSA, and D-H key agreement. Multi-chip standalone module. LunaCA is a hardware crypto engine for identification and authentication (I&A) and digital signing; supports encryption/decryption and random number generation. Its target is certification authority systems that require a secure key generation and signing capability. LunCA is a token based on the PCMCIA standard - now known as PC Card.
37	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar TEL: (847) 576-9066	**KVL 3000** *(when operated in the FIPS mode by selection of the DES algorithm)* (firmware version 1.5)	**Hardware**	11/25/98	***Overall Level:*** **1** -Roles and Services: *Level 2* *-FIPS-approved algorithm:* DES (cert. #5) *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-XL SPFL. Multi-chip standalone module.
36	**Litronic, Inc.** 2030 Main Street Suite 1250 Irvine, CA 92614 http://www.litronic.com -Robert Gray TEL: (949) 851-1085 FAX: (949) 851-8588 info@litronic.com	**Argus/300 Security Adapter** (ID: PN 050-1038)	**Hardware**	11/25/98	***Overall Level:*** **3** *-FIPS-approved algorithms:* DES; SHA-1 (cert. #41) *-Other algorithms:* None. Multi-chip embedded module. Cryptographic Module and Smart Card Reader.
35	**IBM Corp.** 522 South Road Mail Stop P339 Poughkeepsie, NY 12601-5400 http://www.ibm.com/security/ products -Helmy El-Sherif TEL: (914) 435-7033 FAX: (914) 435-4092 helmy@us.ibm.com	**IBM 4758 PCI Cryptographic Coprocessor** (Miniboot Layers 0 and 1) *(When configured for DSS Authentication)* (ID: PN IBM 4758-001, Miniboot 0 version B, Miniboot 1 version B)	**Hardware**	11/25/98	***Overall Level:*** **4** *-FIPS-approved algorithms:* DES (cert. #41); DSA/SHA-1 (cert. #16) *-Other algorithms:* TripleDES (allowed for U.S. Government use), RSA. Multi-chip embedded module. The 4758 is a tamper-responding, programmable, cryptographic PCI card, containing CPU, encryption hardware, RAM, EEPROM, hardware random number generator, time of day clock, firmware, and software.

34	**nCipher, Inc.** 100 Unicorn Park Drive Woburn, MA 01801-3371 http://www.ncipher.com -Greg Dunne TEL: (781) 994-4010 FAX: (781) 994-4001 ussales@ncipher.com	**nFast** **nF75KM 1C, nF150KM 1C, and nF300KM 1C Cryptographic Accelerators** *(Firmware v1.33.1)* *(when operated in the FIPS mode)*	**Hardware**	11/18/98	***Overall Level:*** 2 -Module Interfaces: *Level 3* -Roles and Services: *Level 2** -Software Security: *Level 3* -EMI/EMC: *Level 3* -Self-tests: *Level 2** -Key Management: *Level 2** *(Level 3 is met in these areas when the “FIPS_level3" flag is set during initialization.) *-FIPS-approved algorithms:* DES (cert. #24), DES MAC, DSA/SHA-1 (cert. #11) *-Other algorithms:* TripleDES (allowed for U.S. Government use), Triple DES MAC, CAST, RSA, ElGamal, and D-H key agreement. Multi-chip standalone module. The firmware is used in the nFast series of devices and has been validated on the nFast nF75KM 1C, nF150KM 1C, and nF300KM 1C Cryptographic Accelerators.
33	**Fortress Technologies** 2701 North Rocky Point Dr. Suite 650 Tampa, FL 33607 http://www.fortresstech.com TEL: (813) 288-7388 -Eva Bozoki eva@fortresstech.com -Dennis Joyce dennis@fortresstech.com	**NetFortress™ GVPN** *(Version -1)* *(when factory configured in FIPS mode)*	**Hardware**	11/18/98	***Overall Level:*** 2 *-FIPS-approved algorithms:* DES (cert. #23) *-Other algorithms:* TripleDES (allowed for U.S. Government use), IDEA. Multi-chip standalone module. VPN Encryptor.
32	**Dallas Semiconductor, Inc.** 4401 Beltwood Parkway Dallas, TX 75244-3292 http://www.iButton.com -Mr. Dennis Jarrett TEL: (972) 371-4416 Dennis.Jarrett@dalsemi.com	**DS1954B Cryptographic iButton™** *(ID: B4-V1.02)* *(when using vendor-initialized SHA-1 in transaction group 1)* **Note: This validation has been superseded by validation certificate #41 above, which meets an Overall Level 3.**	**Hardware**	10/28/98	***Overall Level:*** 2 *-Physical Security: Level 3 + EFP* *-EMI/EMC: Level 3* *-FIPS-approved algorithms:* SHA-1 (cert. #8) *-Other algorithms:* MD5, RSA Multi-chip standalone module. Provides hardware cryptographic services (e.g., secure private key storage, high-speed math accelerator for 1024-bit public key crypto, hashing). Services are provided using a single silicon chip packaged in a 16mm stainless steel case. Can be worn or attached to an object for info at point of use. Can withstand harsh outdoor environments and is durable for everyday wear.

31	**Neopost** 30955 Huntwood Ave. Hayward, CA 94544-7084 http://www.neopost.com -Neil Graver TEL: (510) 489-6800 neilgraver@neopostexpress.com	**PostagePlus^{TM} Client Communication Module** (Version 1.0)	**Software**	10/28/98	***Overall Level:*** **1** *-Operating System Security:* Tested as meeting **Level 1** for *Windows95* *-FIPS-approved algorithms:* DES (cert. #38); SHA-1 (cert. #12). *-Other algorithms:* TripleDES *(allowed for U.S. Government use)*, RSA. Multi-chip standalone module. This module is part of the Postage Plus system that provides security services to support the secure accounting and cryptographic functions required to implement the United States Postal Service's Information-Based Indicia Program.
30	**Pitney Bowes, Inc.** 1 Elmcroft Rd. Stamford, CT 06926-0700 http://www.pb.com -Frederick W. Ryan, Jr. TEL: (203) 924-3500 FAX: (203) 924-3385 ryanfw@pb.com	**PC Meter Cryptographic Module** *(Validated only for the DES MAC authenticated services: Credit, Put IBIP Data, and Zeroize Keys)* (Part #P200V, Version ABB)	**Hardware**	10/2/98	***Overall Level:*** **3** *-FIPS-approved algorithms:* DES (cert. #35); SHA-1 (cert. #11). *-Other algorithms:* RSA. Single-chip module. The module provides security services to support the secure accounting and cryptographic functions necessary for value evidencing of electronic transactions, such as the United States Postal Service Information-Based Indicium Program (USPS IBIP).
29	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**LunaCA^{3}** *(For services provided by the listed FIPS-approved algorithms, and Triple DES)* (firmware version 2.2)	**Hardware**	10/2/98	***Overall Level:*** **3** *-FIPS-approved algorithms:* DES (cert. #32); DSA/SHA-1 (cert. #13). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, CAST5, RC2, RC4, MD2, MD5, RSA, and D-H key agreement. Multi-chip standalone module.

28	**nCipher, Inc.** 100 Unicorn Park Drive Woburn, MA 01801-3371 http://www.ncipher.com -Greg Dunne TEL: (781) 994-4010 FAX: (781) 994-4001 ussales@ncipher.com	**nFast** **nF75CA 00, nF150CA 00, and nF300CA 00** **Cryptographic Accelerators** *(Firmware v1.33.1)* *(when operated in the FIPS mode)*	**Hardware**	9/22/98 (nF300CA 00) 11/18/98 (nF75CA 00, nF150CA 00)	***Overall Level:*** **3** -Roles and Services: *Level 3** -Self-tests: *Level 3** -Key Management: *Level 3** *(Level 3 is met in these areas when the “FIPS_level3" flag is set during initialization.) *-FIPS-approved algorithms:* DES (cert. #24), DES MAC, DSA/SHA-1 (cert. #11) *-Other algorithms:* TripleDES (allowed for U.S. Government use), Triple DES MAC, CAST, RSA, ElGamal, and D-H key agreement. Multi-chip standalone module. The firmware is used in the nFast series of devices and has been validated on the nFast nF75CA 00, nF150CA 00, and nF300CA 00 Cryptographic Accelerators.
27	**nCipher, Inc.** 100 Unicorn Park Drive Woburn, MA 01801-3371 http://www.ncipher.com -Greg Dunne TEL: (781) 994-4010 FAX: (781) 994-4001 ussales@ncipher.com	**nFast** **nF75CA 1C, nF150CA 1C, and nF300CA 1C** **Cryptographic Accelerators** *(Firmware v1.33.1)* *(when operated in the FIPS mode)*	**Hardware**	9/22/98 (nF300CA 1C) 11/18/98 (nF75CA 1C, nF150CA 1C)	***Overall Level:*** **3** -Roles and Services: *Level 3** -Self-tests: *Level 3** -Key Management: *Level 3** *(Level 3 is met in these areas when the “FIPS_level3" flag is set during initialization.) *-FIPS-approved algorithms:* DES (cert. #24), DES MAC, DSA/SHA-1 (cert. #11) *-Other algorithms:* TripleDES (allowed for U.S. Government use), Triple DES MAC, CAST, RSA, ElGamal, and D-H key agreement. Multi-chip standalone module. The firmware is used in the nFast series of devices and has been validated on the nFast nF75CA 1C, nF150CA 1C, and nF300CA 1C Cryptographic Accelerators.
26	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Mina Paik Paik.Mina@cylink.com	**Cylink Link Encryptor** **NRZ-L** (Firmware v1.03 and v1.04)	**Hardware**	9/11/98	***Overall Level:*** **2** -Physical Security: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #26); DSA/SHA-1 (cert. #5). *-Other algorithms:* TripleDES (allowed for U.S. Government use), and D-H key agreement. Multi-chip standalone module. Cylink Link Encryptors secure sensitive data transmitted over high-speed, point-to-point communication links. The system supports synchronous, full-duplex data rates up to 2 Mbps over public and private data networks.

25	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Mina Paik Paik.Mina@cylink.com	**Cylink Link Encryptor** **NRZ-H** (Firmware v1.03 and v1.04)	**Hardware**	9/11/98	***Overall Level:*** **2** -Physical Security: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #26); DSA/SHA-1 (cert. #5). *-Other algorithms:* TripleDES (allowed for U.S. Government use), and D-H key agreement. Multi-chip standalone module. Cylink Link Encryptors secure sensitive data transmitted over high-speed, point-to-point communication links. The system supports synchronous, full-duplex data rates up to 2 Mbps over public and private data networks.
24	**V-ONE Corporation, Inc.** 20250 Century Blvd. Suite 300 Germantown, MD 20874 http://www.v-one.com -Mr. Arthur Richer Product Manager TEL: (301) 515-5200 aricher@v-one.com	**SmartPass Virtual Cryptographic Authentication Token (VCAT)** (Version 3.2)	**Software**	9/11/98	***Overall Level:*** **1** -EMI/EMC: *Level 3* *-Operating System Security:* Tested as meeting **Level 1** for *Microsoft Windows95*. *-FIPS-approved algorithm:* DES, SHA-1 (cert. #10) *-Other algorithms:* N/A. Multi-chip standalone module.
23	**GTE Internetworking** 70 Fawcett St. Cambridge, MA 02140 http://www.bbn.com -John Lowry TEL: (617) 873-2435 jlowry@bbn.com	**SafeKeyper™ Signer** *(when initialized to DSA)* (Release 4p)	**Hardware**	9/11/98	***Overall Level:*** **3** *-FIPS-approved algorithm:* DES (cert. #22), DSA/SHA-1 (cert. #9) *-Other algorithms:* RSA, MD2, MD5, Shamir Secret-sharing Algorithm. Multi-chip standalone module.
22	**SPYRUS, Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick (410) 964-6400 BBialick@spyrus.com	**LYNKS Metering Device (LMD)**	**Hardware**	8/13/98	***Overall Level:*** **2** -Physical Security: *Level 3*+EFT -EMI/EMC: *Level 3* *-FIPS-approved algorithms:* SKIPJACK (cert. #1), DSA/SHA-1 (cert. #1) Multi-chip standalone module.

21	**nCipher, Inc.** 100 Unicorn Park Drive Woburn, MA 01801-3371 http://www.ncipher.com -Greg Dunne TEL: (781) 994-4010 FAX: (781) 994-4001 ussales@ncipher.com	**nFast** **nF75KM 00, nF150KM 00, and nF300KM 00 Cryptographic Accelerators** *(Firmware v1.33.1)* *(when operated in the FIPS mode)*	**Hardware**	8/13/98 (nF 150KM 00) 11/18/98 (nF75KM 00, nF300KM 00)	***Overall Level:* 2** -Module Interfaces: *Level 3* -Roles and Services: *Level 2** -Software Security: *Level 3* -EMI/EMC: *Level 3* -Self-tests: *Level 2** -Key Management: *Level 2** *(Level 3 is met in these areas when the "FIPS_level3" flag is set during initialization.) -*FIPS-approved algorithms:* DES (cert. #24), DES MAC, DSA/SHA-1 (cert. #11) -*Other algorithms:* TripleDES (allowed for U.S. Government use), Triple DES MAC, CAST, RSA, ElGamal, and D-H key agreement. Multi-chip standalone module. The firmware is used in the nFast series of devices and has been validated on the nFast nF75KM 00, nF150KM 00, and nF300KM 00 Cryptographic Accelerators.
20	**Entrust Technologies Limited** 750 Heron Road Suite 800 Ottawa, Ontario K1V 1A7 Canada http://www.entrust.com -Marc Laroche TEL: (613) 247-3446 FAX: (613) 247-3450	**Entrust Cryptographic Kernel, V 4.0** *(when operated in the FIPS mode)*	**Software**	7/30/98	***Overall Level:* 1** -EMI/EMC: *Level 3* -*Operating System Security:* Tested as meeting **Level 1** for *Windows95 and WindowsNT 4.0 workstation* (operated in single user mode). -*FIPS-approved algorithms:* DES (cert. #1), DES MAC, DSA/SHA-1 (cert. #10) -*Other algorithms:* TripleDES (allowed for U.S. Government use), RC2, MD5, MD2, HMAC-SHA-1, HMAC-MD5, RSA, CAST, CAST3, CAST5, and D-H key agreement. Multi-chip standalone module. This module is used in the Entrust family of products.
19	**Dallas Semiconductor, Inc.** 4401 Beltwood Parkway Dallas, TX 75244-3292 http://www.iButton.com -Mr. Dennis Jarrett TEL: (972) 371-4416 Dennis.Jarrett@dalsemi.com	**DS1954 Cryptographic iButton™** *(ID: A7-V1.01)* *(when using vendor-initialized SHA-1 in transaction group 1)* **Note: This validation has been superseded by validation certificate #41 above, which meets an Overall Level 3.**	**Hardware**	6/29/98	***Overall Level:* 2** *-Physical Security: Level 3 + EFP* *-EMI/EMC: Level 3* -*FIPS-approved algorithms:* SHA-1 (cert. #8) -*Other algorithms:* MD5, RSA Multi-chip standalone module. Provides hardware cryptographic services (e.g., secure private key storage, high-speed math accelerator for 1024-bit public key crypto, hashing). Services are provided using a single silicon chip packaged in a 16mm stainless steel case. Can be worn or attached to an object for info at point of use. Can withstand harsh outdoor environments and is durable for everyday wear.

18	**Entrust Technologies Limited** 750 Heron Road Suite 800 Ottawa, Ontario K1V 1A7 Canada http://www.entrust.com -Marc Laroche TEL: (613) 247-3446 FAX: (613) 247-3450	**Entrust Cryptographic Kernel, V 3.1** *(when operated in the FIPS mode)*	**Software**	5/11/98	***Overall Level:* 1** -EMI/EMC: *Level 3* -*Operating System Security:* Tested as meeting **Level 1** for *Windows95 and WindowsNT 4.0 workstation* (operated in single user mode). -*FIPS-approved algorithms:* DES (cert. #1), DES MAC, DSA/SHA-1 (cert. #10) -*Other algorithms:* TripleDES (allowed for U.S. Government use), RC2, MD5, MD2, RSA, CAST, CAST3, CAST5, and D-H key agreement. Multi-chip standalone module. This module is used in the Entrust family of products.
17	**GTE Internetworking** 70 Fawcett St. Cambridge, MA 02140 http://www.bbn.com -John Lowry TEL: (617) 873-2435 jlowry@bbn.com	**SafeKeyper™ Signer** *(when initialized to DSA)* (Release 4) **Note: This module is no longer available and has been superseded by certificate #23 above.**	**Hardware**	5/11/98	***Overall Level:* 3** -*FIPS-approved algorithm:* DES (cert. #22), DSA/SHA-1 (cert. #9) -*Other algorithms:* RSA, MD2, MD5, Shamir Secret-sharing Algorithm. Multi-chip standalone module.
16	**Transcrypt International** 4800 NW 1st Street Lincoln, NE 68521 http://www.transcrypt.com -Jim Gilley TEL: (402) 474-4800 FAX: (402) 474-4858 des@transcrypt.com	**SC20-DES, v1.0**	**Hardware**	4/15/98	***Overall Level:* 1** -EMI/EMC: *Level 3* -*FIPS-approved algorithm:* DES (cert. #19) Single-chip module. Encryption module for land mobile radios.
15	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar TEL: (847) 576-9066	**ASTRO XTS 3000 Subscriber Encryption Module** *(when operated in the FIPS mode by selecting the DES algorithm and setting OTAR to inhibited)* (Release R 3.0)	**Hardware**	1/30/98	***Overall Level:* 1** -Roles and Services: *Level 2* -*FIPS-approved algorithm:* DES -*Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-XL SPFL, DVP Multi-chip standalone module. The ASTRO XTS 3000 radio provides portable analog and digital two-radio communications in trunked and conventional radio systems. It is capable of supporting 12.5 kHz digital channels as well as 25 kHz and 30 kHz analog channels. The ASTRO XTS 3000 Subscriber Encryption Module Controller is available as an option for the ASTRO XTS 3000 radios to provide secure communication capabilities.

14	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar TEL: (847) 576-9066	**ASTRO Subscriber Encryption Module** *(when operated in the FIPS mode by selecting the DES algorithm and setting OTAR to inhibited)* (Release R 3.0)	**Hardware**	1/30/98	***Overall Level:* 1** -Roles and Services: *Level 2* *-FIPS-approved algorithm:* DES *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-XL SPFL, DVP Multi-chip standalone module. The ASTRO Saber radio provides portable analog and digital two-radio communications in trunked and conventional radio systems. The ASTRO Spectra radio provides analog and digital two-radio communications in trunked and conventional mobile radio systems. They are each capable of supporting 12.5 kHz digital channels as well as 25 kHz and 30 kHz analog channels.
13	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar TEL: (847) 576-9066	**ASTRO-TAC** **Digital Interface Unit (DIU) Encryption Module Controller (EMC)** *(when operated in the FIPS mode by selection of the DES algorithm)* (version 3.0)	**Hardware**	1/30/98	***Overall Level:* 1** -Roles and Services: *Level 2* *-FIPS-approved algorithm:* DES *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-SPFL Multi-chip standalone module. The ASTRO DIU provides an interface between an analog console and an ASTRO base station or ASTRO-TAC comparator for ASTRO clear and analog two-way radio communications. The DIU EMC is available as an option with ASTRO DIUs to provide encryption capability. The DIU will then support ASTRO encrypted two-way radio communications.
12	**IRE, Inc. (Information Resource Engineering)** 8029 Corporate Drive Baltimore, MD 21236 http://www.ire.com -Joe Schonfeld Product Manager TEL: (410) 931-7500 joes@ire.com	**SafeNet/Dial Secure Modem** *(when operated in 'user with authentication' mode)* (firmware version 2.0)	**Hardware**	12/8/97	***Overall Level:* 2** -EMI/EMC: *Level 3* *-Roles and Services:* Strongest authentication provided when operated in conjunction with the SafeNet/Security Center. *-FIPS-approved algorithm:* DES *-Other algorithm:* ATLAS Multi-chip standalone module.
11	**Motorola, Inc.** Secure Design Center 1301 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar TEL: (847) 576-9066	**Radio Network Controller Encryption Module Controller (RNC EMC)** *(when operated in the FIPS mode by selection of the DES algorithm)* (firmware version D01.00.00)	**Hardware**	11/12/97	***Overall Level:* 1** -Module Interfaces: *Level 3* *-FIPS-approved algorithm:* DES *-Other algorithms:* DES-XL, DVI-XL, DVP-XL, DVI-SPFL Multi-chip standalone module. The RNC 3000 provides data communications between mobile data and host applications in an ASTRO integrated voice and data system. The RNC Encryption Module Controller provides data encryption services for the RNC 3000.

10	**Cylink Corporation** 3131 Jay St P.O. Box 54952 Santa Clara, CA 95056-0952 http://www.cylink.com -Dale Witt dwitt@cylink.com	**Turbo Crypto Card (TCC), v09** (Part#: AB-14094-010-09)	**Hardware**	11/12/97	***Overall Level:*** **1** -EMI/EMC: *Level 3* *-FIPS-approved algorithms:* DES (certs. #11, #12); DSA/SHA-1 (cert. #5). *-Other algorithms:* Diffie-Hellman. Multi-chip embedded module. Turbo Crypto Card is used in a variety of Cylink's host encryption products, including the Secure Frame Unit (SFU) and the Secure Domain Unit (SDU).
9	**IRE, Inc. (Information Resource Engineering)** 8029 Corporate Drive Baltimore, MD 21236 http://www.ire.com -Joe Schonfeld TEL: (410) 931-7500 joes@ire.com	**SafeNet/LAN VPN Encryptor** (firmware version 2.0)	**Hardware**	11/12/97	***Overall Level:*** **2** *-Roles and Services:* Strongest authentication provided when operated in conjunction with the SafeNet/Security Center. *-FIPS-approved algorithm:* DES *-Other algorithm:* ATLAS Multi-chip standalone module.
8	**Chrysalis-ITS** 1688 Woodward Drive Ottawa, Ontario K2C 3R7 Canada http://www.chrysalis-its.com -Blair Canavan VP Sales TEL: (613) 723-5077 FAX: (613) 723-5069 bcanavan@chrysalis-its.com	**Luna 1 PCMCIA Token** *(when operated in the FIPS mode for encryption, decryption, and random number generation)* (firmware version 1.19)	**Hardware**	10/29/97	***Overall Level:*** **2** -EMI/EMC: *Level 3* *-FIPS-approved algorithms:* DES (cert. #13); SHA-1 (cert. #7). *-Other algorithms:* Triple DES *(allowed for U.S. Government use)* CAST, CAST3, MD2, MD5, RSA. Multi-chip standalone module. Chrysalis' Luna 1 is a PC Card that is used to provide generation and storage of symmetric and asymmetric keys, storage of Certificates, and random number generation. It can support up to 15 different users.
7	**Netscape Communications Corporation** 6905 Rockledge Dr., Suite 820 Bethesda, MD 20817 `http://www.netscape.com` -Frank Hecker Netscape Govt. Sales TEL: (301) 571-3907 FAX: (301) 571-3915 fips@netscape.com	**Netscape Security Module 1** *(when operated in the FIPS mode for secure e-mail, certificate management, and password management)* (ID: *fipscm_v1*)	**Software**	8/29/97	***Overall Level:*** **2** *Phys:* **Level 2** met when correctly implementing tamper evident mechanism specified in sec. policy. *O/S:*Tested as meeting **Level 2** w/ *Sun Sparc 5 w/ Sun Solaris v 2.4SE* (ITSEC-rated), and **Level 1** for *MS WindowsNT 4.0 workstation* (operated in single user mode) *-FIPS-approved algorithms:* DES (certs. #6, #10); DSA and SHA-1 (cert. #3). *-Other algorithms:* RSA, RC4, RC5, MD2, MD5. Security module used in various Netscape products.

6	**Mykotronx, Inc.** 357 Van Ness Way Suite 200 Torrance, CA 90501 http://www.rainbow.com/mykoweb/index.htm -Kevin Cook TEL: (310) 533-8100 FAX: (310) 533-0527 kcook@myko.rainbow.com	**Palladium Fortezza Crypto Card** (Part Number 650000)	**Hardware**	6/11/97	***Overall Level:*** **2** -EMI/EMC: *Level 3* *FIPS-approved algorithms:* DSA, SHA-1, Skipjack *Other algorithms:* KEA Multi-chip standalone module.
5	**SPYRUS, Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick (410) 964-6400 BBialick@spyrus.com	**FORTEZZA Crypto Card, v0.2**	**Hardware**	2/7/97	***Overall Level:*** **2** *FIPS-approved algorithms:* DSA, SHA-1, Skipjack *Other algorithms:* KEA Multi-chip standalone module. SPYRUS's FORTEZZA is a PC Card that is used to provide cryptographic services.
4	**National Semiconductor Corporation** (This cryptomodule and NSC's Fortezza business unit have been discontinued.)	**Fortezza PCMCIA Encryption Module** (Part Number 990010947-200)	**Hardware**	10/24/96	***Overall Level:*** **2** *FIPS-approved algorithms:* DSA, SHA-1, Skipjack *Other algorithms:* KEA Multi-chip standalone module.
3	**Entrust Technologies** (formerly Northern Telecom) 750 Heron Road Suite 800 Ottawa, Ontario K1V 1A7 Canada http://www.entrust.com -Marc Laroche TEL: (613) 247-3446 FAX: (613) 247-3450	**Entrust Cryptographic Kernel, V 2.4** *(when operated in the FIPS mode)*	**Software**	9/17/96	***Overall Level:*** **1** (for use with PCs) *FIPS-approved algorithms:* DES, DSA, SHA-1 *Other algorithms:* MD5, MD2, RSA, CAST, CAST3 This module is used in the Entrust family of products.
2	**Motorola, Inc.** Communications Sector 1309 East Algonquin Road Schaumburg, IL 60196 http://www.motorola.com -Geoff Hobar (847) 576-9066	**ASTRO Subscriber Encryption Module**: for ASTRO Radio Product Family (NTN7771D, NTN7772D, NTN7332D, NTN7331D)	**Hardware**	1/19/96	***Overall Level:*** **1** *FIPS-approved algorithms:* DES (CFB mode) *Other algorithms:* Motorola DVP This module is used in the ASTRO Radio Product Family.
1	**Entrust Technologies** (formerly Northern Telecom) 750 Heron Road Suite 800 Ottawa, Ontario K1V 1A7 Canada http://www.entrust.com -Marc Laroche TEL: (613) 247-3446 FAX: (613) 247-3450	**Entrust Cryptographic Module, V 1.9**	**Software**	10/12/95	***Overall Level:*** **1** (for use with PCs) *FIPS-approved algorithms:* DES, DSA *Other algorithms:* CAST, RSA, MD5, MD2 This module is used in the Entrust family of products.

Questions regarding modules/products on the above list should first be directed to the appropriate vendor.

The following three lists are included for historical purposes only. They reflect the various cryptographic implementations which met certain conditions specified in FIPS 140-1, which allowed for a transition from using FS1027 endorsed (and FIPS 140 compliant) implementations to using FIPS 140-1 validated modules. *The three lists in this section should no longer be used by agencies and departments to acquire cryptographic modules.*

● Until January 31, 1997, agencies could acquire implementations that had been submitted for validation under the CMV Program. Since that date, agencies have been required to purchase implementations containing cryptographic modules that have been validated under the CMV Program (or meet the next bulleted condition below).

● Until June 30, 1997, agencies could also acquire implementations that had either (1) received a Federal Standard 1027 endorsement from NSA or (2) had been affirmed by the vendor as meeting FIPS 140 (both predecessors to FIPS 140-1). The affirmation letter must have been received by NIST prior to June 30, 1994. The following two lists indicate implementations which met these requirements:

Cryptographic Modules that have received FS 1027 Endorsement from the National Security Agency.

FIPS 140-1 specifies that "For up to three years following June 30, 1994, equipment with cryptographic modules complying to FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard* (formerly FS 1027), may be purchased in lieu of equipment with modules that comply with FIPS 140-1. These modules either shall have been endorsed by the National Security Agency (NSA) as complying to Federal Standard 1027, or shall be affirmed in writing by the manufacturer as complying to FIPS 140." [FIPS 140-1, *Security Requirements for Cryptographic Modules*, Paragraph 14, Implementation Schedule, page 3]. The following products received Federal Standard 1027 Endorsement from the National Security Agency. These products were acceptable in lieu of products validated under the CMV Program until June 30, 1997. This list should no longer be used by a Federal department or agency that is purchasing equipment.

Vendor	Product Endorsed	Comments
California Microwave, Inc.	Model CD-5800	Product Discontinued.
Hughes Network Systems 10450 Pacific Center Court San Diego, CA 92121 TEL: (619) 453-7007 Ext. 4701	LC76A-DS1; LC76; LC76CF DKD	Product Discontinued; still providing support for existing parts.
ATT Paradyne	Infolock Model 2811-13	Product Discontinued; ATT Paradyne formerly Paradyne Corporation.
Racal-Guardata, Inc. 480 Spring Park Pl., Ste 900 Herndon, VA 22070 TEL: (703) 471-0892	DC64-1027, 10-02A01(V.35), 10-02A00 (RS232C); 10-02A02 (V.11)	None

Racal-Guardata, Inc.
480 Spring Park Pl., Ste 900
Herndon, VA 22070
TEL: (703) 471-0892
	10-02A30; 10-02A31;
	10-02A32; 10-02A50;
	10-02A70; 10-02A71;
	10-02A100; 10-02A101
		None

Atlantic Research Corp.	Model Number FES-100 (Acorn)	Product Discontinued
Cylink 910 Hermosa Court Sunnyvale, CA 94087 TEL: 1-800-600-5858 http://www.cylink.com	CIDEC-HS, CIDEC-LS	CIDEC-LS now CIDED-LSi
Datotek	Model CIPHERBIT 1027-13	Product Discontinued
Fairchild Communications and Electronics Co. Fairchild Industries, Inc.	Burst Encryption Unit	Product Discontinued

Technical Communications Corp.
100 Domino Drive
Concord, MA 01742
TEL: (508) 287-5100
	CIPHER X 5000-1027-X.25;
	CIPHER X 5000-1027;
	CSD 3324A
		CIPHER X 5000-1027-X.25
		now CIPHER X 5000 A-PS;
		CIPHER X 5000-1027
		now CIPHER X 5000 A-PT;
		CSD 3324A now CSD 3324E

SPAR Communcications Group 2811 Airpark Drive Santa Maria, CA 93455 TEL: (805) 928-2581	CT-5000	None
Computer Sciences Corp. 4600 Powder Mill Rd. Beltsville, MD 20705 TEL: (410) 684-3600	SECOM 2010	None
Digitech Telecommunications, Inc. 551 Madison Ave., Tenth Floor New York, NY 10022 TEL: (212) 935-4380	LS-1027	None
Motorola, Inc. Communications Sector 1309 East Algonquin Rd. Schaumburg, IL. 60196 TEL: (312) 397-1000	Key Variable Loader; Console Interface Unit; Saber I, II, III, Portable Radio; Systems Saber I & III Portable Radio; Spectra Mobile Radio, A4, A5, A7, A9 Control Heads; Smartnet Spectra Mobile Radio, C2, C5, C7, C9 Control Heads; Spectra Desktop; Key Management Controller; MSF5000 Securenet Conventional Base Stations/Repeaters	None

Cryptographic Modules with Vendor Affirmation to FIPS 140 (Predecessor to FIPS 140-1)

FIPS 140-1 specifies that "For up to three years following June 30, 1994, equipment with cryptographic modules complying to FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard* (formerly FS 1027), may be purchased in lieu of equipment with modules that comply with FIPS 140-1". [FIPS 140-1, *Security Requirements for Cryptographic Modules*, Paragraph 14, Implementation Schedule, page 3]. The following list identifies those products whose vendors have claimed conformance to FIPS 140 through written affirmation. The list is ordered based on the date of the affirmation letter. Products on this list were acceptable in lieu of products validated under the CMV Program until June 30, 1997. This list should no longer be used by a Federal department or agency that is purchasing equipment.

Vendor	Product	Description
Racal-Guardata 48000 Spring Park Pl. Suite 900 Herndon, Va. 22070 TEL (305) 846-4942 FAX (703) 437-9333	DC64-1027C, DC64HS	DC64-1027C is an NSA endorsed encryption device (USGEID #00000041). DC64HS is vendor affirmed to meet FIPS 140. Affirmation letter dated 11/26/90.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Motorola Systems Saber 1 Handie Talkie FM Radio	Vendor affirmed to FIPS 140 when equipped with one of the following options: H388, H795, H868, H869. Affirmation letter dated 6/12/91.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	SPECTRA Two Way Secure Voice Conventional Voice Radio	Vendor affirmed to FIPS 140 when equipped with the W391option, the W496 option and one of the following DES options:W388, W795, W968, and W969. Affirmation letter dated 6/12/91.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	MSF 5000 SECURENET Digital Capable Conventional Base Stations and Repeaters	Vendor affirmed to FIPS 140 when equipped with the C514 option, the C557 option and one of the following DES options: C388 and C795. Affirmation letter dated 6/12/91.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Spectra Securenet Capable Desktop Station	Vendor affirmed to FIPS 140 when equipped with option L938 and one of the following DES options: L388, L795 L968, L969. Affirmation letter dated 6/12/91.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Advanced Securenet Key Management Controller	Vendor affirmed to FIPS 140. Affirmation letter dated 6/12/91.

Cypher Communications Technology, Inc. 702 Russel Ave. Suite 450 Gaithersburg, Md. 20877 TEL (301) 590-9314 FAX (301) 590-9346	CYCOM SCI	Vendor affirmed to FIPS 140. Also placed on the Treasury Qualified Products List for message authentication devices. Affirmation letter dated 9/6/91.
Ericcson GE Mobile - Communications, Inc. Mountain View Rd. Lynchburg, VA 24502 TEL (804) 528-7000	Aegis M-PA	Handheld land mobile radio. Vendor claims conformance to FIPS 140 when equipped with DES encryption option. Affirmation letter dated 3/20/92.
Racal-Guardata 480 Spring Park Place Suite 900 Herndon, Va. 22070 TEL (703) 471-0892 FAX (703) 437-9333	Datacryptor 64E	Vendor affirmed to FIPS 140. DES-based X.25 packet encryption device. Key management in accordance with ANSI X9.17. Affirmation letter dated 3/24/92.
Cylink, Inc. 310 North Mary Ave. Sunnyvale CA. 94086 TEL (408) 735-5800 http://www.cylink.com	CyNet Manager KMS/EMS	Vendor affirmed to FIPS 140. Based on DES based Cidec-HS encryptor. Includes an ANSI X9.17 key distribution center. Affirmation letter dated 4/30/92.
Cylink, Inc. 310 North Mary Ave. Sunnyvale CA. 94086 TEL (408) 735-5800 http://www.cylink.com	Cidec-Hsi	Vendor affirmed to FIPS 140. Upgrade of Cidec-HS. (Cidec-HS is under the FS 1027 endorsement program (USEGID #00000025). Incorporates DES. Vendor affirmed to FIPS 140 when configured for either manual key mgmt. or ANSI X9.17 key management. Affirmation letter dated 4/30/92.
Racal-Guardata 480 Spring Park Place Suite 900 Herndon, Va. 22070 TEL (703) 471-0892 FAX (703) 437-9333	Datacryptor 64 and Datacryptor 64C	Vendor affirmed to FIPS 140. Standalone DES-based link encryptors designed to support secure communications at speeds up to 64Kbps. Affirmation letter dated 8/3/92.
Cylink, Inc. 310 North Mary Ave. Sunnyvale CA. 94086 TEL (408) 735-5800 http://www.cylink.com	Cidec-LS (and Cidec-MS)	Vendor affirmed to FIPS 140. FS 1027 endorsement program, (USEGID # 00000039). Affirmation letter dated 8/12/92.

Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Key Variable Loader, Console Interface Unit Saber I, II, III Portable Radio Systems Saber III Portable Radio	Vendor affirmed to FIPS 140. These products under NSA endorsement program. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Saber ATS	Vendor affirmed to FIPS 140 when equipped with one of the following DES options: H388, H795. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Spectra Desktop Station	Vendor affirmed to FIPS 140 when equipped with the L938 option and the L795 DES option. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Portable Repeater II	Vendor affirmed to FIPS 140 when equipped with the H391 option and the following DES options: H388 and H795. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Securenet Decoding Receiver	Vendor affirmed to FIPS 140 when equipped with the C557 option, a physical security kit, and one of the following DES options: C388 and C795. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	MTS2000 radio	Vendor affirmed to FIPS 140 when equipped with the following DES options: H388, H795, NTN 1301, NTN 1303. Affirmation letter dated 6/30/94.
Motorola Inc. 1309 East Algonquin Road Schaumburg, Ill. 60196 TEL (312) 397-1000	Astro Portable radio	Vendor affirmed to FIPS 140 when equipped with one of the following DES options: NTN7771A, NTN7772A, NTN7332A, NTN7331A. Affirmation letter dated 6/30/94.

● From the effective date of FIPS 140-1 (June 30, 1994) until January 31, 1996, agencies could accept vendor written affirmation claiming an implementation’s conformance to FIPS 140-1. NIST maintains vendors’ letters of written affirmation. Agencies shall no longer acquire cryptographic modules after January 31, 1996 which have *only* received written vendor affirmation.

Cryptographic Modules with Vendor Affirmation to FIPS 140-1.

The following list identifies those products whose vendors have claimed conformance to FIPS 140-1 through written affirmation. The list is ordered based on the date of the affirmation letter. Written affirmation could only be accepted in lieu of validation until January 30, 1996. This list should no longer be used by a Federal department or agency that is purchasing equipment.

Vendor	Product	Description
Racal-Guardata 480 Spring Park Place Suite 900 Herndon, VA 22070 TEL (703) 471-0892 FAX (703) 437-9333	Master Access Gateway Master Secure Gateway, Access Gateway Expansion Chassis, Secure Gateway Expansion Chassis, Dedicated Network Security Manager, CAT-2001H, CAT-3001H, CAT-3002H and CAT-2001P. Datacryptor 64 MS1 (DC64MS1), Datacryptor 64 MS2 (DC64MS2).	Vendor claims conformance to FIPS 140-1. No FIPS 140-1 level is specified. Affirmation letter is dated 1/6/94. Affirmation letter for Datacryptor products is dated 9/13/95.
Litronic 2950 Redhill Ave. Costa Mesa, CA TEL (714) 545-6649	ARGUS/300	Vendor claims conformance to FIPS 140-1. Model is claimed to FIPS 140-1 Level 3. Affirmation letter is dated 5/4/94.
Via Crypt 2104 West Peoria Avenue Phoenix, Arizona 85029 TEL (602) 944-0773 FAX (602) 943-2601	D150 Cryptographic Engine, D300 Security Module, D350 Cryptographic Adapter, D355 Cryptographic Adapter, D360 Cryptographic Adapter.	Vendor claims conformance to FIPS 140-1. The D150 model is claimed to Level 1. Models D300, D350, D355 and D360 are claimed to Level 3. Affirmation letter is dated 6/14/94.
IRE, Inc. 8029 Corporation Drive Baltimore, Md. 21236 TEL (410) 931-7500 FAX (410) 931-7524	SC3000W+, SC3000+, 96M, 96M-2, 96M-SF, CLR/CRYPT, MAC, USERID, MON, MA, AX100, AX200, AX400, AX500, 96NX-SC, 24JX, 96MS, 192MN, MHS, MHS-V, MHS-VC, HS, HS-V, HS-VC, MAX	Vendor claims conformance to FIPS 140-1. No FIPS 140-1 Level specified for models. Affirmation letter is dated 6/30/94.
Motorola, Inc. Communications Sector 1309 East Algonquin Road Schaumburg, IL 60196 TEL (312) 397-1000	MTS2000 Series Portable Radio, Astro Saber Portable Radio Module Kits, Astro Spectra Mobile Encryption Module Kits, Astro Digital Interface Unit Encryption Cartridge, Advanced Securnet Key Management Controller.	Vendor claims conformance to FIPS 140-1. All models are claimed to FIPS 140-1 Level 1. Affirmation letter is dated 6/30/94.
Secured Communications Canada 93 Incorporated 35 Freshway Drive Concord, Ontario Canada L4K 1R9 TEL (905) 738-5300 FAX (905) 738-6919	Session Key Data Security PCMCIA TYPE II Hardware based Security Device.	Vendor claims conformance to FIPS 140-1. Model is claimed to FIPS 140-1 Level 1. Affirmation letter is dated 10/11/94.

Western Datacom Co. Inc. 959-B Basset Rd. Westlake, OH 44145 TEL (216) 835-1510 FAX (216) 835-9146	CryptoCom V.32bis/V.34	Vendor claims conformance to FIPS 140-1. Model is claimed to FIPS 140-1 Level 3 (excluding Class B EMI requirements). Affirmation letter is dated 4/14/95.
Elementrix Technologies, Inc. 850 Third Ave. New York, NY. 10022 TEL (212) 888-8879 FAX (212) 935-3882	POTP Secure FTP, POTP Secure FTP Server for Unix, POTP Secure Mail.	Vendor claims conformance to FIPS 140-1. Model is claimed to FIPS 140-1 Level 4. Affirmation letter is dated 1/29/95.
Netscape Communications Corp. 6701 Democracy Blvd., Suite 300 Bethesda, Md. 20817 TEL (301) 571-9477 FAX (301) 571-9619	Netscape Navigator, Netscape Commerce Sever, Netscape Proxy Server, Netscape News Server	Vendor claims conformance to FIPS 140-1. Models are claimed to meet or exceed FIPS 140-1 Level 1. Affirmation letter is dated 1/29/95.